AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Black Apple iPhone in blue protective case
Silver Apple iPhone in black protective case
Black Apple iPhone in clear protective case,
Black Apple iPhone in black protective case

Case No. 3:20 mj 128

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. §§ 846 & 841(a)(1)	Conspiracy to possess with intent to distribute a controlled substance

The application is based on these facts:

See Attached Affidavit.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA TIMOTHY J. WALLACE, HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: 3-10-20

Judge's signature

City and state: Dayton, Ohio

Sharon L. Ovington, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF: Black Apple iPhone in blue protective case, Silver Apple iPhone in black protective case, Black Apple iPhone in clear protective case, and Black Apple iPhone in black protective case.	Case No. _____

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Timothy J. Wallace, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I, Timothy J. Wallace, am a Special Agent of Homeland Security Investigations (HSI), United States Department of Homeland Security. As such, I set forth the following in support of a search warrant for one (1) Black Apple iPhone in blue protective case (Subject Device 1); one (1) Silver Apple iPhone in black protective case (Subject Device 2); one (1) Black Apple iPhone in clear protective case (Subject Device 3); one (1) Black Apple iPhone in black protective case (Subject Device 4). Subject Devices 1 through 4 are currently within the Southern District of Ohio in the custody of HSI.

2. I am an employee of Homeland Security Investigations assigned to the Cincinnati Resident Office. I have been a Special Agent with HSI since July 2009. I attended and graduated from the basic agent training course in Brunswick, Georgia and have received extensive training

in the investigation of narcotics trafficking and financial crimes from Homeland Security Investigations, as well as ongoing in-service training.

3. Since February 2018, I have been assigned to the HSI Border Enforcement Security Task Force (BEST) in Dayton, Ohio.

4. As a Special Agent for HSI, I am charged with the duty of enforcing among other Titles, the Controlled Substance Act, Title 21, United States Code, together with other assigned duties as imposed by federal law.

5. By virtue of my employment with HSI, I perform and have performed various tasks which include, but are not limited to:

a. Functioning as a surveillance agent for the primary purpose of observing and movements of drug traffickers and those suspected of trafficking in drugs;

b. Functioning as a case agent which entails the supervision of specific aspects of drug investigations; and,

c. Tracing and tracking monies and assets gained by drug traffickers from the illegal sale of drugs.

6. This Affidavit seeks the issuance of a search warrant. There is probable cause that Marcus Lushound **DENNIS** and Edward Lamont **JONES**, violated Title 21 U.S.C. § 846 and 841 (b)(1)(A) (conspiracy to possess with intent to distribute 400 grams or more of fentanyl). All of the details of the investigation are not included in this Affidavit, rather only information necessary to establish probable cause to search Subject Devices 1 through 4. There is probable cause to believe that evidence of these violations is contained within the cellular telephones as further described and depicted in Attachment A.

7. The information contained in this affidavit comes from my personal knowledge and facts relayed to me by other law enforcement officers. Unless otherwise noted, when I assert that a statement was made, I received the information from a law enforcement officer who provided the information to me, either verbally or in a written report. The officer providing me with the information may have received the information by way of personal knowledge or from another source.

PROBABLE CAUSE

8. Together with agents and officers of the HSI Cincinnati Border Enforcement Security Task Force ("BEST"), I am currently involved in the investigation related to the drug offenses believed to have been committed by Marcus Lushound DENNIS (**DENNIS**) and Edward Lamont JONES (**JONES**). Based upon the investigation to date, there is probable cause to believe that **DENNIS** and **JONES** violated Title 21 U.S.C. § 846 and 841 (b)(1)(A) (conspiracy to possess with intent to distribute 400 grams or more of fentanyl).

9. On February 14, 2020, HSI in conjunction with the Miami Valley Bulk Smuggling Task Force (hereinafter collectively referred to as "Agents") received information from a confidential source (CS) in reference to a large-scale fentanyl operation occurring between California and Columbus, Ohio. CS advised agents that an unknown black male who was living in Columbus, had possession of numerous kilogram quantities of suspected fentanyl. CS advised agents that the unknown subject drove a black Chrysler bearing Ohio license plate number HUP4181.

10. Agents conducted a registration check and learned the vehicle was registered to **DENNIS**, who showed a home address in the greater Columbus area. A criminal history check showed **DENNIS** had a previous drug related case filed by the Drug Enforcement

Administration.

11. On February 16, 2020, CS advised agents that **DENNIS** would be traveling from Columbus to the area of South Vienna, Ohio, with two kilograms of suspected fentanyl. CS stated **DENNIS** might utilize a female to deliver the fentanyl. Agents with the Miami Valley Bulk Smuggling Task Force responded to I-70 in the area of mile marker 59 through 66 to conduct surveillance.

12. At approximately 1:30 pm on February 16, 2020, Trooper Weeks, assisting with surveillance in a marked Ohio State Highway Patrol vehicle, observed **DENNIS'** Chrysler 200 bearing Ohio license plate HUP4181 pass Trooper Weeks traveling west. Trooper Weeks was directed to stop the vehicle for reasonable suspicion of drug activity.

13. Upon approach, Trooper Weeks identified DENNIS as the driver and the passenger as **JONES**, who produced a State of California driver's license. During the traffic stop, Trooper Weeks deployed his trained drug-detection canine partner, who conducted a free air sniff of the vehicle. Trooper Weeks canine, Ryo, gave a positive alert to the vehicle and a probable cause search was conducted. Trooper Weeks advised no contraband was located in the vehicle.

14. During the encounter with **DENNIS** and **JONES**, Trooper Weeks located and seized Subject Devices 1 through 4 as evidence.

15. As Trooper Weeks was on the traffic stop, CS contacted agents and advised **DENNIS** had told someone, possibly a female, to pull over at the BP Gas Station located on exit 59 of I-70. Agents pulled into that area with unmarked police vehicles and conducted surveillance at about the same time.

16. During surveillance, agents observed a female, later identified as **RISOR**, acting

nervously while sitting in her vehicle, a white Chevy Malibu bearing Ohio license plate FWC3161. After observing **RISOR** continually move and park in multiple different locations within the BP Gas Station parking lot, agents with the Miami Valley Bulk Smuggling Task Force, approached **RISOR** at her vehicle.

17. During contact with **RISOR**, Trooper Pohlabel deployed his trained drug-detection canine partner, Sahra, for a free air sniff of **RISOR's** vehicle. Sahra gave a positive alert to the vehicle for the presence of a narcotic odor and a probable cause search was conducted. During the search of the vehicle, agents located approximately two kilograms of suspected fentanyl hidden in the carpet liner of the trunk area.

18. Agents also located a holstered Smith & Wesson M&P 380 Shield EZ loaded with a round in the chamber in the center console of **RISOR**'s vehicle. **RISOR** had her valid Franklin County Concealed Carry Handgun permit with her as well.

19. Trooper Pohlabel advised **RISOR** of her constitutional rights. **RISOR** stated she understood her rights and was willing to give agents a statement. **RISOR** stated she traveled to **DENNIS'** residence, located at 3802 Preserve Crossing Blvd, Gahanna, OH 43230, to meet with **DENNIS**. **RISOR** stated **DENNIS** and **JONES** were both in the residence when she arrived. **RISOR** stated **DENNIS** told her he would pay her $500 to drive her vehicle to meet with someone in the area of exit 59 off I-70.

20. **RISOR** said thought the trip was illicit in nature but denied knowing she was transporting drugs. **RISOR** stated that when she arrived at **DENNIS'** house she left her keys on the counter and went to the bathroom for few minutes. **RISOR** said that when she came out of the bathroom, they (**DENNIS** and **JONES**), were ready to leave and told her to start driving. **RISOR** stated they told her they would be following in **DENNIS'** vehicle.

21. **RISOR** provided agents with written consent to search her cell phone. During a cursory search, agents observed multiple text messages and phone calls between **DENNIS** and **RISOR** that took place on February 16, 2020 both prior to and during the smuggling venture.

22. At approximately 6:00 pm on February 16, 2020, agents executed a state search warrant at **DENNIS'** residence located at 3802 Preserve Crossing Blvd, Gahanna, OH 43230. During the search, agents located a safe that was bolted to the floor in the master bedroom closet of **DENNIS'** residence. Found within the safe were three (3) additional kilograms of suspected fentanyl, a folder containing a birth certificate from the State of Michigan for Marcus Lushound **DENNIS**, Social Security Card or Marcus Lushound **DENNIS**, and an Ohio Interim Document – Driver License for Marcus Lushound **DENNIS** bearing his address of 3802 Preserve Crossing Blvd, Gahanna, OH 43230 with an issuance date of December 26, 2019.

23. I believe that Subject Devices 1 through 4 may contain evidence of communication between **DENNIS**, **JONES**, **RISOR**, and additional known and unknown co-conspirators and other evidence related to drug trafficking by these individuals. I request permission to search the electronic data stored in Subject Devices 1 through 4 to locate any other evidence of drug trafficking activity that may be inside.

24. In my experience, cellular phones are often used by criminals to carry out their business. Criminals often use the phones to communicate (either by voice, text message, or internet-based communication accessed by the phone) with customers, suppliers, and associates about pending criminal activity. It is also common to find photographs of their criminal associates stored on the phones, as well as photos of weapons, drugs, money, or assets associated with their illegal activity. Criminals will often store phone numbers for their associates in the cellular phone, and sometimes use alias or code names for those entries. Electronic evidence

stored on the phone also can show who used a particular cellular phone, because criminals often use prepaid phones or fake subscriber names when obtaining the phone from the service provider. Criminals commonly have multiple phones at a given time, with certain phones used to communicate with particular individuals or for specific purposes. By searching the data stored on Subject Devices 1 through 4, I believe evidence of **DENNIS** and **JONES**' criminal activity may be revealed.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

25. The property to be searched is one (1) Black Apple iPhone in blue protective case (Subject Device 1); one (1) Silver Apple iPhone in black protective case (Subject Device 2); one (1) Black Apple iPhone in clear protective case (Subject Device 3); and, one (1) Black Apple iPhone in black protective case (Subject Device 4). Subject Devices 1 through 4 are currently located and held by HSI at the HSI Evidence Room, located at 9875 Redhill Dr, Blue Ash, OH 45242 (and within the Southern District of Ohio). Subject Devices 1 through 4 are depicted and described in Attachment A.

26. The applied-for warrant would authorize the forensic examination of Subject Devices 1 through 4 for the purpose of identifying electronically stored data particularly described in Attachment B.

27. Subject Devices 1 through 4 are currently in the lawful possession of HSI. Subject Devices 1 through 4 came into HSI's possession after the Devices were seized during the course of the aforementioned traffic stop.

28. Based on my training and experience, I know that Subject Devices 1 through 4 have been stored in a manner in which the contents are, to the extent material to this

investigation, in substantially the same state as they were when the Subject Devices first came into the possession of HSI.

TECHNICAL TERMS

29. Based upon my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved

in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

30. Based on my training, experience, and research, I know that Subject Devices 1 through 4 are cellular telephones, and that most modern cellular telephones have capabilities that allow them to serve as "a wireless telephone, digital camera, portable media player, GPS navigation device, and PDAs." In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

31. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensic tools.

32. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Subject Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on these Subject Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

33. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of Subject Devices 1 through 4 consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to, computer-assisted scans of the entire medium that might expose many parts of the Subject Devices to human inspection in order to determine whether it is evidence described by the warrant.

34. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

35. For these reasons, I submit that this affidavit supports probable cause for a search warrant authorizing the examination of Subject Devices 1 through 4 described in Attachment A, to seek the items described in Attachment B, which are evidence of violation of Title 21 U.S.C. § 846 and 84l (b)(l)(A) (conspiracy to possess with intent to distribute 400 grams or more of fentanyl).

Respectfully submitted,

Timothy J. Wallace, Special Agent
Homeland Security Investigations

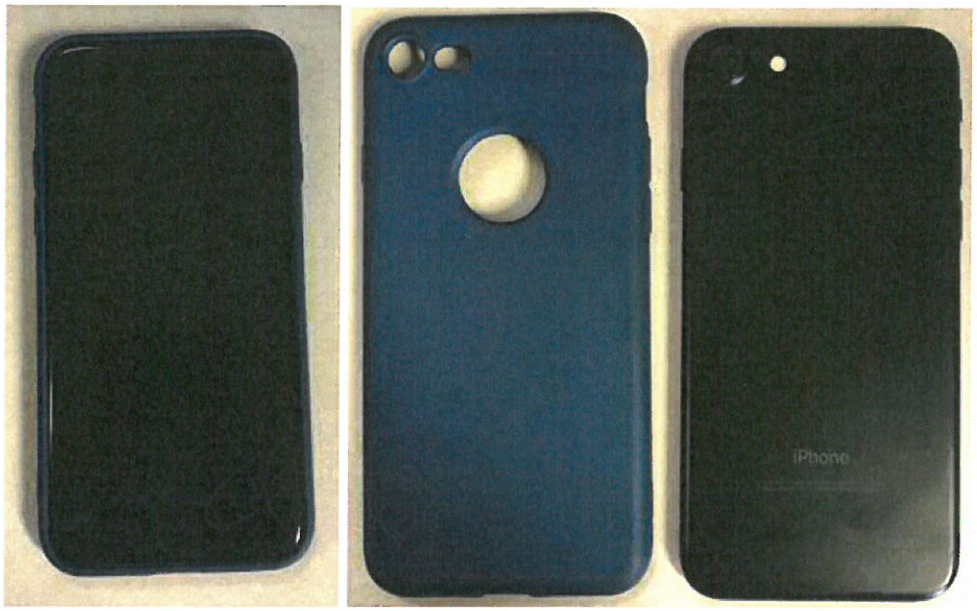
Subscribed and sworn to before me on March 10, 2020.

Honorable Sharon L. Ovington
United States Magistrate Judge

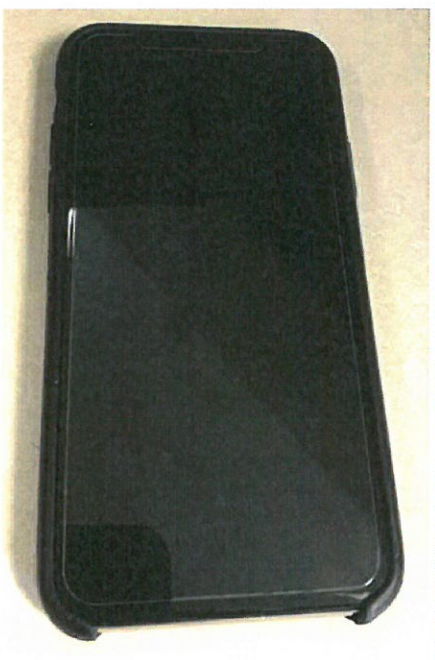
ATTACHMENT A

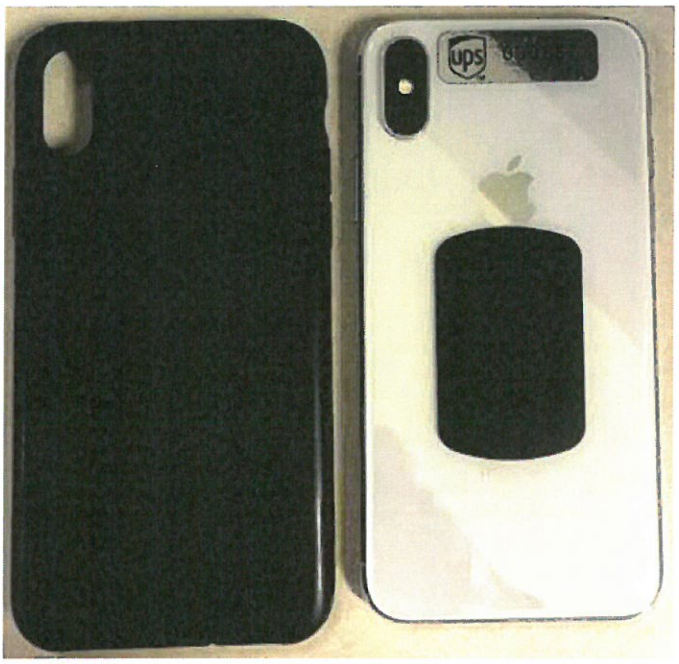
This warrant applies to the following devices:

1. One (1) Black Apple iPhone in blue protective case, together with all electronic devices, including Subscriber Identity Modules, or SIM cards, contained therein (Subject Device 1). Subject Device 1 is currently located in the custody of HSI at the HSI Evidence Room, located at 9875 Redhill Dr, Blue Ash, OH 45242 (and within the Southern District of Ohio). It is depicted in the photographs below:

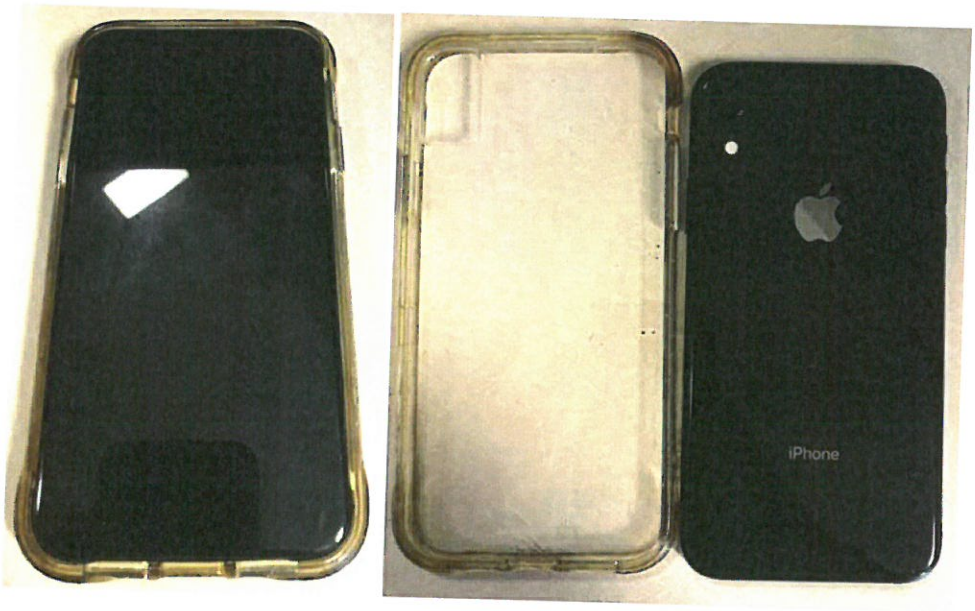


2. One (1) Silver Apple iPhone in black protective case, together with all electronic devices, including Subscriber Identity Modules, or SIM cards, contained therein (Subject Device 2). Subject Device 2 is currently located in the custody of HSI at the HSI Evidence Room, located at 9875 Redhill Dr, Blue Ash, OH 45242 (and within the Southern District of Ohio). It is depicted in the photographs below:

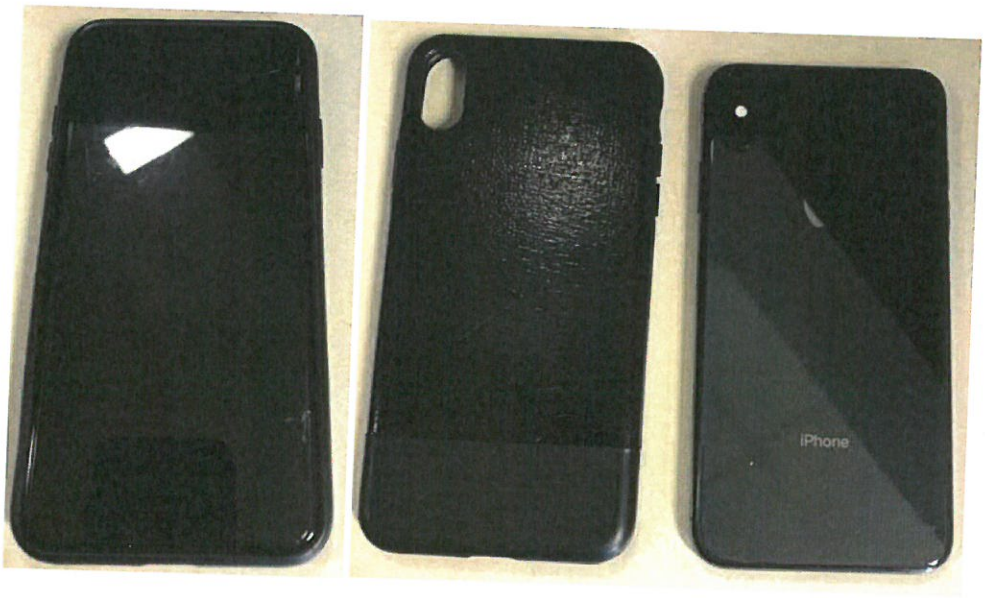




3. One (1) Black Apple iPhone in clear protective case, together with all electronic devices, including Subscriber Identity Modules, or SIM cards, contained therein (Subject Device 3). Subject Device 3 is currently located in the custody of HSI at the HSI Evidence Room, located at 9875 Redhill Dr, Blue Ash, OH 45242 (and within the Southern District of Ohio). It is depicted in the photographs below:



4. One (1) Black Apple iPhone in black protective case, together with all electronic devices, including Subscriber Identity Modules, or SIM cards, contained therein (Subject Device 4). Subject Device 4 is currently located in the custody of HSI at the HSI Evidence Room, located at 9875 Redhill Dr, Blue Ash, OH 45242 (and within the Southern District of Ohio). It is depicted in the photographs below:



This warrant authorizes the forensic examination of Subject Device 1, Subject Device 2, Subject Device 3, and Subject Device 4 for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Subject Devices described in Attachment A that relate to violations of Title 21 U.S.C. § 846 and 841 (b)(l)(A), involving Marcus Lushound DENNIS and Edward Lamont JONES, including but not limited to:

a. Lists of contacts and related identifying information;

b. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

c. Any information related to transferring, transporting of currency to include banking information;

d. Any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);

e. Any information recording DENNIS' and JONES' schedule or travel, such as the use of hotel rooms or other lodging, rental cars, or airline information; all bank records, checks, credit card bills, account information, and other financial records.

f. Evidence of communication and association between DENNIS' and JONES' co-conspirators, including "WhatsApp" or other cell phone applications used to communicate, text messages, photographs, email, Facebook, or other social media, phone call logs, and stored phone numbers;

g. Evidence of user attribution showing who used or owned the Subject Devices at the time the items described in this warrant were created, edited, or deleted, such

as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

h. Records evidencing the use of any Internet Protocol addresses to communicate with Facebook or any other website, including:

i. Records of Internet Protocol addresses used;

j. Records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.